**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

Claim 1. (Currently Amended): A method of detecting a rogue access point by a client comprising the steps of:

directing a packet from ~~a supplicant~~the client to a network through a[[n]] first access point;

receiving a network response packet by the ~~supplicant~~ client from the first access point;

determining that the first access point is a rogue access point by the client based on the network response packet received from the access point in being in nonconformity with predetermined expectations;

authenticating the client through a valid access point to the network subsequent to determining that the first access point is a rogue access point; and

reporting the first access point as a rogue access point by the client to the network through the valid access point.

Claim 2. (Currently Amended): The method of claim 1, further comprising the step of authenticating the ~~supplicant~~ client to the network.

Claims 3 and 4. (Cancelled)

Claim 5. (Currently Amended): The method of claim 1 wherein the predetermined expectations comprise data traffic conforming with [[IEEE]]Institute of Electrical and Electronic Engineers 802.1X standards.

Claim 6. (Previously Presented): The method of claim 1 wherein the predetermined expectations comprise a mutual authentication to the network, wherein nonconformity is determined by a failure of the mutual authentication.

Claim 7. (Currently Amended): The method of claim 6 wherein the mutual authentication comprises:

issuing a challenge from [[the]] an authentication server to the client;

issuing a counter-challenge from the client to the authentication server;

wherein mutual authentication fails at the counter-challenge since the first access point's username and password are not found in the authentication server's database.

Claim 8. (Currently Amended): The method of claim 6 wherein the mutual authentication comprises:

directing a message containing identity credentials from the ~~supplicant~~client, through the access point, to an authentication server;

validating the identity credentials of the ~~supplicant~~ client using the authentication server;

forwarding a send key from the authentication server to the ~~supplicant~~ client through the first access point;

independently deriving a session key from the send key and the identity credentials by the ~~supplicant~~ client and the authentication server;

encrypting data packets between the ~~supplicant~~ client and the authentication server using the derived session key.

Claim 9. (Original): The method of claim 8 wherein the credentials are a username/password combination.

Claim 10. (Currently Amended): The method of claim 8 further comprising:

prior to the step of directing, sending a start message from the ~~supplicant~~ client to the first access point;

sending an identity request message from the first access point to the ~~supplicant~~client; and

wherein the step of directing a message comprises sending an identity response message containing the identity credentials ~~form~~ from the ~~supplicant~~ client to the first access point in response to the identity request message, and forwarding the identity response message from the first access point to the authentication server.

Claim 11. (Currently Amended): The method of claim 10 wherein the authentication server is a ~~RADIUS~~Remote Authentication Dial-In User Service server and wherein the identity response message is in the form of a ~~RADIUS~~Remote Authentication Dial-In User Service access request, wherein the method further comprises the steps of:

responding to the ~~RADIUS~~Remote Authentication Dial-In User Service access request with a ~~RADIUS~~Remote Authentication Dial-In User Service challenge from the authentication server to the ~~supplicant~~client; and responding from the ~~supplicant~~ client to the ~~RADIUS~~Remote Authentication Dial-In User Service challenge according to the ~~RADIUS~~Remote Authentication Dial-In User Service protocol.

Claim 12. (Currently Amended): The method of claim 11 wherein the steps of validating and forwarding comprise sending the ~~supplicant~~ client a ~~RADIUS~~Remote Authentication Dial-In User Service accept message and wherein the send key comprises an MicroSoft-Microsoft Point-to-Point Encryption ~~MS-MPPE~~ Send-key.

Claim 13. (Original): The method of claim 8 wherein the step of forwarding a send key comprises supplying key length and key index to specify encryption parameters for the session key.

Claim 14. (Original): The method of claim 10 wherein the encryption parameters are based on one of a 40/64-bit and a 104/128-bit key.

Claim 15. (Currently Amended): The method of claim 8 further comprising the initial step of configuring the client as a supplicant in a device mode where the identity credentials are stored on a network card for non-interactive authentication by a user.

Claim 16. (Currently Amended): The method of claim 8 further comprising the initial step of configuring the client as a supplicant in a network logon mode where the identity credentials are integrated into a network logon to enable a single sign-on for network authentication and [[PC]]personal computer network logon.

Claim 17. (Currently Amended): The method of claim 8 further comprising the initial step of establishing authenticator support comprising:

configuring the valid access point to use one of 40/64-bit and 104/128-bit [[WEP]]Wired Equivalent Privacy mode; and

providing the valid access point with the authentication server address and encryption scheme to be used for communication.

Claim 18. (Currently Amended): The method of claim 8 further comprising the initial step of establishing the authentication server comprising:

setting up a user database selected from at least one of a local database and a network database; and

setting up the valid access point as a network access server.

Claim 19. (Currently Amended): The method of claim 8 wherein the ~~supplicant~~client, valid access point and authentication server are part of a wireless local area network.

Claim 20. (Currently Amended): The method of claim 8 wherein the ~~supplicant~~client, valid access point and authentication server are part of a hard-wired local area network.

Claim 21. (Currently Amended): A client configured ~~with~~ as a supplicant for detecting a rogue access point comprising:

means for directing a packet from the supplicant to a network through a[[n]] first access point;

means for receiving a network response packet by the supplicant from the first access point;

means for determining whether the first access point is a rogue access point based on the network response packet received from the access point being in nonconformity with predetermined expectations;

means adapted for reporting the first access point as a rogue access point through a ~~valid~~ second access point that the client is able to authenticate via the means for directing, the means for receiving and the means for determining.

Claim 22. (Currently Amended): The client of claim 21 further comprising means for authenticating the supplicant to the network, if the second access point is determined to be a valid network access point.

Claims 23 and 24 (Cancelled).

Claim 25. (Currently Amended): The client of claim 21 wherein the predetermined expectations comprise data traffic conforming with [[IEEE]]Institute of Electrical and Electronic Engineers 802.1X standards.

Claim 26. (Previously Presented): The client of claim 1 wherein the predetermined expectations comprise a mutual authentication to the network, wherein non-conformity is determined by a failure of the mutual authentication.

Claim 27. (Currently Amended): The client of claim 21 wherein the means for mutual authentication comprises:

means for directing a message containing identity credentials from the supplicant, through the second access point, to an authentication server;

means for validating the identity credentials of the supplicant using the authentication server;

means for forwarding a send key from the authentication server to the supplicant through the second access point;

means for independently deriving a session key from the send key and the identity credentials by the supplicant and the authentication server;

means for encrypting data packets between the supplicant and the authentication server using the derived session key.

Claim 28. (Previously Presented): The client of claim 27 wherein the credentials are a username/password combination.

Claim 29. (Currently Amended): The client of claim 27 further comprising:

means for sending a start message from the supplicant to the second access point prior to the means for directing;

means for sending an identity request message from the second access point to the supplicant; and

wherein the means for directing a message comprises means for sending an identity response message containing the identity credentials form the supplicant to the second access point in response to the identity request message, and means for forwarding the identity response message from the second access point to the authentication server.

Claim 30. (Currently Amended): The client of claim 29 wherein the authentication server is a ~~RADIUS~~Remote Authentication Dial-In User Service server and wherein the identity response message is in the form of a ~~RADIUS~~Remote Authentication Dial-In User Service access request, wherein the arrangement further comprises:

means for responding to the ~~RADIUS~~Remote Authentication Dial-In User Service access request with a ~~RADIUS~~Remote Authentication Dial-In User Service challenge from the authentication server to the supplicant;

and means for responding from the supplicant to the ~~RADIUS~~Remote Authentication Dial-In User Service challenge according to the ~~RADIUS~~Remote Authentication Dial-In User Service protocol.

Claim 31. (Currently Amended): The client of claim 29 wherein the means for validating and forwarding comprise means for sending the supplicant a ~~RADIUS~~Remote Authentication Dial-In User Service accept message and wherein the send key comprises an MicroSoft-Microsoft Point-to-Point Encryption ~~MS-MPPE~~-Send-key.

Claim 32. (Previously Presented): The client of claim 27 wherein the means for forwarding a send key comprises means for supplying key length and key index to specify encryption parameters for the session key.

Claim 33. (Previously Presented): The client of claim 32 wherein the encryption parameters are based on one of a 40/64-bit and a 104/128-bit key.

Claim 34. (Currently Amended): The client of claim 27 wherein the supplicant, second access point and authentication server are part of a wireless local area network.

Claim 35. (Currently Amended): The client of claim 27 wherein the supplicant, second access point and authentication server are part of a hard-wired local area network.